Information Warfare

Lisa Jaworski
(703) 824-5418
Communications & Engineering Solutions Group
System Engineering

SAIC®
An Employee-Owned Company

What Is Information Warfare?

"Those actions intended to protect, exploit, corrupt, deny, or destroy information or information resources in order to achieve a significant advantage, objective, or victory over an adversary."

John I. Alger

Dean, School of Information Warfare & Strategy

National Defense University

What Is Happening?

- Proliferation of Malware in the Wild
- Increased DoS & DDoS Attacks
  - Immediate & Time Delayed Attacks
  - Home Users Employed as Zombies
  - Can Be Combined With Other Attacks
- Intelligence Gathering Largely Unnoticed
- DNS Attacks for Propaganda
- Web Site Defacement
- VPN Hijacking
- Social Engineering

More Reality Bites

- Government Needs Industry Cooperation to Fight IW
- Serious Lack of Information Security Expertise
- False Sense of Security from Products
- Majority Don’t Follow Minimal Security Practices
- Not Cost Effective for Vendors to Test Security
- IW Will Escalate Proportional to US Response
- Script Kiddies Ride Coat Tails of Those Motivated by Ideology, Creed, & Greed

Targeted Industries

- Military
- Civilian Federal & State Governments
- Banking & Finance
- Power
- Water Supply
- Medical
- Transportation
- Communications
- Public Safety
- Security Specialists, e.g., CERT

What Is Needed to Fight Back?

- Management Support for Security
- Organized Approach
- Take Care of High Priority Activities First
- Assign Data Ownership for Control Purposes
- Budget
- Question Security Provided by Your ISP

What Are You Protecting?

- People
  - Employees
  - Customers
  - Primary & Secondary Stakeholders
- Data
- Computing Resources
- Physical Facilities
- Reputation & Customer Confidence
- Stock Price
- Your Job

What Are High Priority Activities?

- Install Firewall & IDS, If Not Already Present
  - Internet Access Points & Multiple In-Line Firewalls
  - Between Operational Facilities & Schools
  - Guard More Sensitive Departments
- Standard Secure Configuration Templates
  - Install All Necessary Security Patches
  - Disable All Unnecessary Services
  - Change Default Passwords
  - Other
- Remove All Unauthorized Modems
- Painfully Limit Vendor Access

More High Priority Activities

- Restrict Access to Privileged Accounts
- Personal Firewalls & Hard Drive Encryption on All Laptops & Executive Machines
- Increase Audit Logging & Perform Daily Reviews
- Consider Tripwire for Routers
- Choose Strong Encryption Algorithms
- Background Checks for Key Sensitive Positions
- Background Checks & Fingerprints for Non-Employee Workforce Members

Physical Security

- Lock Down Data Center, Wiring Closets, Security Administration Areas, Test Labs, & Other Sensitive Areas
- Stringent Visitor Controls
- Stringent Physical Access Controls Beyond Visitor Reception
- Sweep Executive Suites for Bugs Regularly
- Suspicious Packages & Mail Room Security
- Teach Employees to Challenge Unknown Persons

Account Administration Is Key

- Minimal Privileges for Each Job Function
- Delete/Suspend Accounts for Terminated Employees
- Consider Context-Based Access Control
- Strong Authentication for Dialup
- Do Not Use Round Numbers for Standard Activity Intervals, e.g., 92 Days for Password Aging
- Automatic Logoff
- Password Reuse Controls
- Other

Security Training & Awareness

- Management, Technical, Support, & Janitorial Staff
- Specialized Training for Security Administration, Incident Response, Evidence Collection, & Disaster Recovery
- Foster Responsible Attitude
- Promote Realization of Individual Accountability
- Relate Security to National & Corporate Goals
- Program Must Be Continuous
  - New Hire Orientation
  - Annual Refresher Training
  - Memos & Newsletters

Security Training Topics

- Develop Sensitivity to Social Engineering
  - Telephone
  - E-mail Subject Lines
  - Visitor Control
  - Janitorial Staff
  - Senior Management
- Virus Prevention, Detection, & Eradication
- Incident Reporting
- E-mail Retention & Expectations for Privacy
- Verify Identity of Originator Via Digital Certificates
- Use of Security Mechanisms & Assurance Measures
- Proper Actions During Bomb Scare
- Dumpster Diving

Necessary Documents

- Security Policy
- Incident Response Plan*
- Contingency Plan*
- Users' Security Guide
- Security Administration Procedures*
  - Perimeter Defense
  - Audit Logging & Review
  - Account Administration

* As-Needed Basis & Burn/Shred Old Versions

Organizational Structure

- Information Security Officer (ISO)
- Incident Response Team
- Disaster Recovery Team
- Security Administration Team
- Test & Evaluation Team (Lab Environment)
- External Connectivity Control Board
- Server Security Control Board
- Security Guards
- Video Surveillance Attendants

Conclusions

- This Is Real, Folks!!
- Anyone Who Uses a Computer Is Affected
- Constant Vigilance Is Necessary
- Protect, Detect, React, & Recover

Resources

- Information Warfare – Winn Schwartau
- Cyber Attacks During the War on Terrorism: A Predictive Analysis – Institute for Security Technology Studies, Dartmouth College
- Tangled Web – Richard Power
- Hacking Exposed – Stuart McClure, Joel Scambray, & George Kurtz
- Secrets & Lies – Bruce Schneier